

SEGURANÇA CIBERNÉTICA

PARTE 1

Gilberto Gonzaga de Figueiredo

ESPECIALISTA EM ADMINISTRAÇÃO E SEGURANÇA
DE SISTEMAS COMPUTACIONAIS

ESPECIALISTA EM CYBERCRIME E CYBERSECURITY -
PREVENÇÃO E INVESTIGAÇÃO DE CRIEMES DIGITAIS

ISO – Information Security Officer

DPO – Data Protection Officer

ECSA – Endian Certificate



SEGURANÇA CIBERNÉTICA

1. PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

- EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA
- VALOR DA INFORMAÇÃO ALINHAMENTO ESTRATÉGICO DA SEGURANÇA AOS NEGÓCIOS
- INVESTIMENTO NECESSÁRIO PARA GARANTIR A PROTEÇÃO DOS DADOS
- PLANO DE CIBERSEGURANÇA (CYBERSECURITY PLAN)

SEGURANÇA CIBERNÉTICA

Segurança Cibernética - Trata de um conjunto de ações que são aplicadas sobre pessoas, tecnologias e processos para garantir a segurança das informações contra ataques que usam as redes de dados como meio para conseguir acesso indevido a sistemas de informação e etc.

PROPRIEDADES E PRINCÍPIOS DE SEGURANÇA

A segurança de um sistema de computação pode ser expressa através de algumas propriedades fundamentais [Amoroso, 1994]:

Segurança da Informação

Confidencialidade

Integridade

Disponibilidade

Autenticidade

Não repúdio

PROPRIEDADES E PRINCÍPIOS DE SEGURANÇA

- **Confidencialidade** : os recursos presentes no sistema só podem ser consultados por usuários devidamente autorizados a isso;
- **Integridade** : os recursos do sistema só podem ser modificados ou destruídos pelos usuários autorizados a efetuar tais operações;
- **Disponibilidade** : os recursos devem estar disponíveis para os usuários que tiverem direito de usá-los, a qualquer momento.

Além destas, outras propriedades importantes estão geralmente associadas à segurança de um sistema:

PROPRIEDADES E PRINCÍPIOS DE SEGURANÇA

- **Autenticidade** : todas as entidades do sistema são autênticas ou genuínas; em outras palavras, os dados associados a essas entidades são verdadeiros e correspondem às informações do mundo real que elas representam, como as identidades dos usuários, a origem dos dados de um arquivo, etc;
- **Irretratabilidade** : Todas as ações realizadas no sistema são conhecidas e não podem ser escondidas ou negadas por seus autores; esta propriedade também é conhecida como irrefutabilidade ou não-repudiação.

ATAQUE CIBERNÉTICO

Ataque Cibernético - Um ataque cibernético é faz referência a qualquer tipo de ação ofensiva com objetivo de atingir sistemas de informação de computadores, infraestruturas de sistemas, redes de computadores ou dispositivos de uso pessoal.

VALOR DA INFORMAÇÃO

A informação é hoje um dos bens mais preciosos tanto para pessoas físicas quanto para as empresas, na atualidade assume uma importância que só cresce a cada dia, a informação pode fazer a diferença entre o fracasso e o sucesso de uma organização, a informação é fundamental para a descoberta e introdução de novas tecnologias, exploração de novas as oportunidades de investimento e de crescimento. A informação é um orientador das oportunidades e sinalizadora das ameaças a que a empresa esta sujeita, a informação ajuda a reduzir as incertezas em tomadas de decisões de forma que, as decisões tomadas tenham resultados mais favoráveis.

VALOR DA INFORMAÇÃO

Fatores a serem considerados sobre o valor da Informação:

- O valor da informação pode variar conforme seu contexto e sua aplicação;
- Informações corretas e adequadas ajudam na tomada de decisões;
- Informações incorretas ou mesmo ultrapassadas podem acarretar em perdas financeiras para as empresas diante de um mercado competitivo;
- Informações em excesso podem ser prejudiciais aos negócios ou acarretar em perda de tempo;
- Informações que não possuem um impacto real para os negócios não são consideradas tão valiosas.

EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Com o crescimento das Redes de Computadores e aumento constante de usuários na Internet, está havendo também um aumento constante de ações criminosas através das redes de comunicação, como exemplo disso podemos citar: Manipulações de caixas bancários, nos sistemas de telecomunicação, pirataria de programas de computador entre outros tipos de crimes possíveis de serem cometidos através das redes de dados. Desde então, os tipos ataques têm evoluído e novas técnicas são desenvolvidas a cada dia, diante dessa realidade os ciber criminosos vem se tornado cada vez mais audaciosos e elevando o número de crimes.

INVESTIMENTO NECESSÁRIO PARA GARANTIR A PROTEÇÃO DOS DADOS

Não há um valor pré-definido para o investimento em segurança dos dados, os investimentos a serem feitos vai depender de uma série de fatores como por exemplo: Tamanho e porte da empresa, tipo de negócios, qual pilar da informação será prioridade, análise e avaliação de risco, apetite ao risco, nível de importância dado a cada tipo de informação, tecnologia envolvida entre outros.

O valor da Informação vai depender do quanto ela é importante para os negócios, ela pode ajudar a aumentar os lucros ou conseguir uma vantagem competitiva.

PLANO DE CIBERSEGURANÇA (CYBERSECURITY PLAN)

Um plano de Ciber Segurança compreende os processos e as ações que devem ser tomadas para proteger os sistemas, dados e qualquer ativo importante para os negócios. Um plano de Segurança Cibernética é um roteiro de proteção, que deve ser elaborado com base num bom planejamento e na definição de vários procedimentos que devem ser executados mediante as várias situações que envolve a proteção dos dados e até situações de recuperação em caso de falhas.

PLANO DE CIBERSEGURANÇA (CYBERSECURITY PLAN)

Para criar um bom plano de Segurança devemos:

- Determinar o que deve ser protegido
- Definir os ativos;
- Determinar quem são os proprietários dos ativos;
- Determinar quais são as ameaças;
- Decidir quais são os agentes de ameaça;
- Obter opiniões dos especialistas;
- Definir o impacto;
- Realizar uma análise e avaliação de riscos;
- Definir o apetite ao risco;
- Mitigar o risco inaceitável;
- Implementar controles;
- Criar documentação necessária a cada situação;
- Entre outras.

Um plano de Ciber Segurança além de melhorar os níveis de segurança, também deve constar o que fazer em caso de falhas.

PLANO RECUPERAÇÃO DE DESASTRE

Plano Recuperação de desastre (disaster recovery) - Compreende um conjunto de políticas e procedimentos que devem ser seguidos para ajudar na recuperação ou continuação da infraestrutura de tecnologia e dos sistemas mais importantes para as empresas na ocorrência de um desastre natural ou provocado pelo homem.

Um dos fatores primordiais nesse processo, é o backup das informações mais importantes para a continuidade dos negócios, diante dessa realidade existem dois fatores que devem ser bem planejados:

- **RPO**: objetivo do ponto de recuperação
- **RTO**: objetivo de tempo de recuperação

PLANO RECUPERAÇÃO DE DESASTRE

RTO – Representa o tempo máximo aceitável desde o último Backup, o RTO determina o que é considerado uma perda de dados aceitável entre o último backup e o momento da interrupção do serviço, esse período é definido pela organização.

RPO - Representa o tempo máximo de parada aceitável entre a interrupção do serviço até o momento da sua restauração. O RPO determina espaço de tempo aceitável de inatividade dos serviço em caso de falha, esse período é definido pela organização.

AMEAÇAS À CONTINUIDADE DOS NEGÓCIOS

Alguns exemplos de ameaças para a continuidade dos negócios são:

- Falhas nos sistemas tecnológicos;
- Catástrofes naturais;
- Fraudes;
- Roubo;
- Inadequação às legislações vigentes;

PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

Um Plano de Continuidade de Negócios são procedimentos documentados que devem seguidos para garantir que, caso situações de crise venham a acontecer, que a empresa esteja preparada para respostas rápidas e eficientes, prontas para serem colocadas em prática de forma a dar continuidade aos processos mais importantes para os negócios.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Uma PSI é um documento extremamente importante no contexto da Ciber Segurança, uma PSI tem como objetivo ajudar no gerenciamento da segurança nas empresas, um PSI estabelece regras e padrões para auxiliar na proteção das informações.

Trata-se de um conjunto de padrões, normas e diretrizes a serem seguidas por todos os colaboradores que utilizam infraestrutura de TI das empresas. O objetivo principal da PSI é ajudar a garantir a proteção das informações das empresas contra eventuais ameaças que possam prejudicar sua operação.

POLÍTICA DE SEGURANÇA

As decisões relacionadas à segurança que você toma, ou não toma, sendo um administrador, em grande parte determinam o quão segura ou insegura sua rede é ou será. Quanta funcionalidade sua rede oferece e o quão fácil ela é de ser utilizada. Porém, você não pode tomar boas decisões sem determinar primeiro quais são suas metas de segurança.

Até que você determine suas metas de segurança, você não poderá fazer uso efetivo de qualquer coleção de ferramentas de segurança, simplesmente porque você não saberá o que conferir ou quais restrições impor. Suas metas serão determinadas em grande parte pelos seguintes pontos chaves:

- Serviços oferecidos versus segurança provida
- Facilidade de uso versus segurança
- Custo de segurança versus risco de perda

POLÍTICA DE SEGURANÇA

Serviços oferecidos versus segurança provida - Cada serviço oferecido aos usuários apresenta um próprio risco de segurança. Para alguns serviços, o risco excede em valor o benefício do serviço e o administrador pode escolher eliminar o serviço em lugar de tentar deixá-lo seguro.

POLÍTICA DE SEGURANÇA

Facilidade de uso versus segurança : O sistema mais fácil de usar permitiria acesso a qualquer usuário e não requereria senha; isso quer dizer, não haveria nenhuma segurança. Requerer senhas torna o sistema um pouco menos conveniente, mas mais seguro. Requerer senhas geradas em dispositivos que as alteram toda vez que você se loga, faz o sistema até mesmo mais difícil para uso, mas muito mais seguro.

POLÍTICA DE SEGURANÇA

Custo de segurança versus risco de perda : Existem muitos custos referentes à segurança:

monetário - O custo de comprar hardware de segurança e software como firewalls e geradores de senhas descartáveis)

desempenho - Cifragem e decifragem levam tempo, e facilidade de uso como mencionado acima.

Também há muitos níveis de risco:

- **perda de privacidade** (a leitura de informação por indivíduos sem autorização)
- **perda de dados** (a corrupção ou deleção de informação) e a perda de serviço por exemplo, o preenchimento do espaço de armazenamento de dados, uso de recursos computacionais, e negação de acesso à rede). Cada tipo de custo deve ser pesado contra cada tipo de perda. Suas metas devem ser comunicadas a todos os usuários, ao pessoal da operação e aos gerentes através de um conjunto de regras de segurança, chamadas "política de segurança".

POLÍTICA DE SEGURANÇA

Quem deveria estar envolvido quando for definida uma Política de Segurança?

- O administrador de segurança do site
- O pessoal técnico da tecnologia de informação (por exemplo, o pessoal do centro de computação);
- Os administradores de um determinado grupo de usuários dentro da organização (por exemplo, divisões empresariais, departamento de ciência de computação dentro de uma universidade, etc.);
- Um grupo responsável por respostas a incidente de segurança;
- Os representantes dos grupos de usuários afetados pela política de segurança;
- Responsável pela administração;
- Um representante para a deliberação legal (se apropriado), e demais responsáveis pela segurança da informação.

POLÍTICA DE SEGURANÇA

As características de uma boa política de segurança são:

- Deve ser implementável através de procedimentos de administração de sistema, publicando diretrizes sobre uso aceitáveis, ou outros métodos apropriados;
- Deve ser reforçado com o uso de ferramentas de segurança apropriadas e com sanções, onde a prevenção atual não é tecnicamente possível;
- Tem de definir claramente as áreas de responsabilidade para os usuários, administradores, e gerência.

POLÍTICA DE SEGURANÇA

Os componentes de uma boa política de segurança incluem:

- Compra de Tecnologia de computador que especifica a característica de segurança exigida ou a preferida. Estes devem suprir a compra de políticas e de diretrizes existentes;
- Uma Política Privada, a qual define expectativas razoáveis de privacidade, serão definidos limites aceitáveis para características como monitoramento de correio eletrônico, logs das teclas digitadas, e acesso aos arquivos de usuários;
- Uma política de acesso que define os direitos de acesso e privilégios necessários para proteger recursos, evitando assim a perda ou revelação de informação, além de especificar as diretrizes aceitáveis para usuários, pessoal da operação e gerência. Uma política de acesso deve prover também diretrizes para conexões externas, comunicações de dados, conexões de dispositivos a rede e adição de novos softwares aos sistemas. Ela também deve especificar qualquer mensagem de notificação exigida (por exemplo, as mensagens de conexões devem prover advertências sobre o uso autorizado e a monitoração da linha, e não simplesmente dizer "Olá seja muito bem vindo");
- Uma política de responsabilidade que define as responsabilidades dos usuários, pessoal da operação e gerência. A política de responsabilidade também precisa especificar uma capacidade de auditoria e prove diretrizes para a manipulação de incidentes (o que fazer e quem contactar se uma possível intrusão for descoberta);

POLÍTICA DE SEGURANÇA

Os componentes de uma boa política de segurança incluem:

- Uma política de autenticação que estabelece confiança por uma política efetiva de senhas, estabelecendo diretrizes para autenticação remota e o uso de dispositivos de autenticação (por exemplo, senhas descartáveis e os dispositivos que as geram);
- Uma declaração de disponibilidade que fixa as expectativas de usuários pela disponibilidade de recursos. Ela pode se destinar a características de redundância e recuperação, bem como especificar horas operacionais e períodos de manutenção. Também pode incluir informação de contato sobre relatório do sistema e fracassos da rede;
- Um sistema de tecnologia de informação & política de manutenção da Rede que descreve como manutenção interna e externa é permitida para as pessoas dirigirem e acessarem a tecnologia. Um tópico importante a ser ressaltado aqui é quando a manutenção remota é permitida e como tal acesso é controlado;
- Uma política de informação de violações a qual indica quais tipos de violações (por exemplo, privacidade e segurança interna e externa) devem ser informadas e para quem serão feitos os relatórios. Uma atmosfera não ameaçadora e a possibilidade de informação anônima resultarão em uma maior probabilidade de que uma violação seja informada se for descoberta;

POLÍTICA DE SEGURANÇA

Os componentes de uma boa política de segurança incluem:

- Informação de suporte que provê aos usuários, pessoal e gerência uma informação de contato para cada tipo de política de violação;
- Diretrizes de como manipular questões sobre um incidente de segurança, ou informação que pode ser considerada confidencial ou proprietária;
- Referências cruzadas para procedimentos de segurança e informação relacionada, como políticas de companhia e leis governamentais e regulamentos.

PLANO DE SEGURANÇA

Um plano de segurança deve definir:

- Uma lista dos serviços de rede que serão oferecidos;
- Quais áreas da organização proverão os serviços;
- Quem terá acesso a esses serviços;
- Como será provido o acesso;
- Quem administrará esses serviços, etc.

RESOLUÇÃO DE QUESTÕES

RESOLVA AS QUESTÕES PROPOSTAS
SOBRE OS ASSUNTOS ANTERIORES.

SEGURANÇA CIBERNÉTICA

AMEAÇAS, VULNERABILIDADES E TIPOS DE ATAQUES

- INTERCEPTAÇÃO DE TRÁFEGO & MAPEAMENTO DE REDES
- ATAQUES E VULNERABILIDADES DE APLICAÇÕES WEB CÓDIGOS MALICIOSOS
- WIRELESS HACKING

AMEAÇAS

Como ameaça, pode ser considerada qualquer ação que coloque em risco as propriedades de segurança do sistema. Exemplos de ameaças às propriedades básicas de segurança:

- Ameaças à confidencialidade;
- Ameaças à integridade;
- Ameaças à disponibilidade.

AMEAÇAS À INTEGRIDADE

Um processo alterar as senhas de outros usuários, instalar programas, drivers ou módulos de núcleo maliciosos, visando obter o controle do sistema, roubar informações ou impedir o acesso de outros usuários;

AMEAÇAS À CONFIDENCIALIDADE

Um processo vasculhar as áreas de memória de outros processos, arquivos de outros usuários, tráfego de rede nas interfaces locais ou áreas do núcleo do sistema, buscando dados sensíveis como números de cartão de crédito, senhas, e-mails privados, etc.

AMEAÇAS À DISPONIBILIDADE

Um usuário alocar para si todos os recursos do sistema, como a memória, o processador ou o espaço em disco, para impedir que outros usuários possam utilizá-lo.

AMEAÇAS

- Obviamente, para cada ameaça possível, devem existir estruturas no sistema operacional que impeçam sua ocorrência.
- As ameaças podem ou não se concretizar, dependendo da existência e da correção dos mecanismos construídos para evitá-las ou impedi-las.
- As ameaças podem se tornar realidade à medida em que existam vulnerabilidades que permitam sua ocorrência.

VULNERABILIDADE

Uma vulnerabilidade é um defeito ou problema presente na especificação, implementação, configuração ou operação de um software ou sistema, que possa ser explorado para violar as propriedades de segurança do mesmo.

ATAQUE

Ato de utilizar (ou explorar) uma vulnerabilidade para violar uma propriedade de segurança do sistema.



TIPOS DE ATAQUE

- **Interrupção** - consiste em impedir o fluxo normal das informações ou acessos; é um ataque à disponibilidade do sistema;
- **Interceptação** - consiste em obter acesso indevido a um fluxo de informações, sem necessariamente modificá-las; é um ataque à confidencialidade;
- **Modificação** - consiste em modificar de forma indevida informações ou partes do sistema, violando sua integridade;
- **Fabricação** - consiste em produzir informações falsas ou introduzir módulos ou componentes maliciosos no sistema; é um ataque à autenticidade.

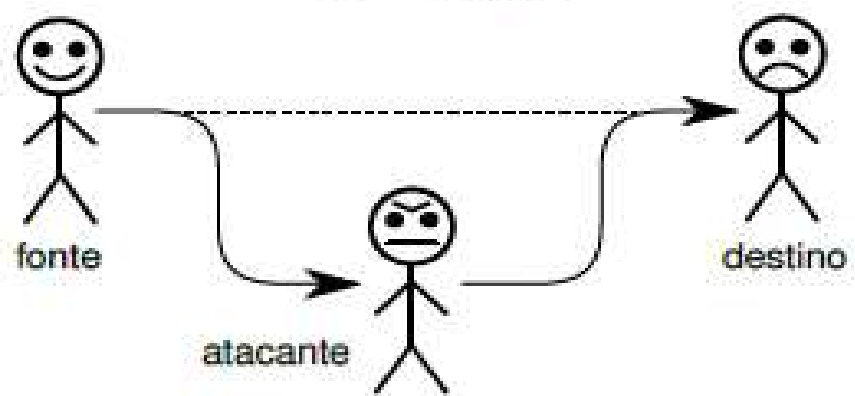
interrupção



interceptação



modificação



fabricação



ATAQUES PODEM SER

- **Passivos** - Visam capturar informações confidenciais;
- **Ativos** - Visam introduzir modificações no sistema para beneficiar o atacante ou impedir seu uso pelos usuários válidos;
- **Locais** - Quando executados por usuários válidos do sistema;
- **Remotos** - Quando são realizados através da rede, sem fazer uso de uma conta de usuário local. Um programa especialmente construído para explorar uma determinada vulnerabilidade de sistema e realizar um ataque é denominado exploit.

WIRELESS HACKING

Ação de identificar e explorar vulnerabilidades em um sistema de computador ou rede, utilizando-se das redes sem fio.

WIRELESS HACKING

Exemplos de tipos de ataques que podem ocorrer em redes Wi-Fi:

- **Engenharia Social;**
- **WLAN Scanners;**
- **Wardriving;**
- **Man in the Middle;**
- **Ponto de Acesso Falso;**
- **Ataque de Engenharia Elétrica;**
- **MAC Spoofing;**
- **Ataque de Senhas;**
- **Ataques de Dicionário;**
- **Força bruta;**
- **Ataques Sniffers;**
- **Denial of Service (DoS);**
- **Port Scanning;**
- **Ataques ao ARP;**
- **Smurf e DHCP**

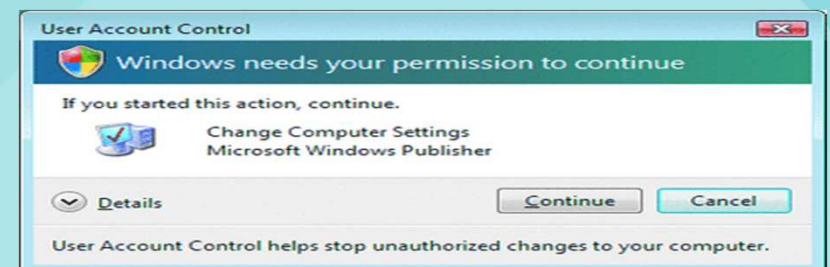
PRINCÍPIOS ESPECÍFICOS DE SEGURANÇA

- **Privilégio mínimo**
- **Mediação completa**
- **Default seguro**
- **Economia de mecanismo**
- **Separação de privilégios**
- **Compartilhamento mínimo**
- **Projeto aberto**
- **Proteção adequada**
- **Facilidade de uso**
- **Eficiência**
- **Elo mais fraco**



PRIVILÉGIO MÍNIMO

Todos os usuários e programas devem operar com o mínimo possível de privilégios ou permissões de acesso. Dessa forma, os danos provocados por erros ou ações maliciosas intencionais serão minimizados.



MEDIAÇÃO COMPLETA

Mediação completa : todos os acessos a recursos, tanto diretos quanto indiretos, devem ser verificados pelos mecanismos de segurança. Eles devem estar dispostos de forma a ser impossível contorná-los.

DEFAULT SEGURO

O mecanismo de segurança deve identificar claramente os acessos permitidos; caso um certo acesso não seja explicitamente permitido, ele deve ser negado. Este princípio impede que acessos inicialmente não-previstos no projeto do sistema sejam inadvertidamente autorizados.

ECONOMIA DE MECANISMO

O projeto de um sistema de proteção deve ser pequeno e simples, para que possa ser facilmente e profundamente analisado, testado e validado.

SEPARAÇÃO DE PRIVILÉGIOS

Sistemas de proteção baseados em mais de um controle são mais robustos, pois se o atacante conseguir burlar um dos controles, mesmo assim não terá acesso ao recurso. Um exemplo típico é o uso de mais de uma forma de autenticação para acesso ao sistema (como um cartão e uma senha, nos sistemas bancários).

COMPARTILHAMENTO MÍNIMO

Mecanismos compartilhados entre usuários são fontes potenciais de problemas de segurança, devido à possibilidade de fluxos de informação imprevistos entre usuários. Por isso, o uso de mecanismos compartilhados deve ser minimizado, sobretudo se envolver áreas de memória compartilhadas. Por exemplo, caso uma certa funcionalidade do sistema operacional possa ser implementada como chamada ao núcleo ou como função de biblioteca, deve-se preferir esta última forma, pois envolve menos compartilhamento.

PROJETO ABERTO

A robustez do mecanismo de proteção não deve depender da ignorância dos atacantes; ao invés disso, o projeto deve ser público e aberto, dependendo somente do segredo de poucos itens, como listas de senhas ou chaves criptográficas. Um projeto aberto também torna possível a avaliação por terceiros independentes, provendo confirmação adicional da segurança do mecanismo.

PROTEÇÃO ADEQUADA

Cada recurso computacional deve ter um nível de proteção coerente com seu valor intrínseco (Que está dentro, que faz parte). Por exemplo, o nível de proteção requerido em um servidor Web de serviços bancário é bem distinto daquele de um terminal público de acesso à Internet.

FACILIDADE DE USO

O uso dos mecanismos de segurança deve ser fácil e intuitivo, caso contrário eles serão evitados pelos usuários.

EFICIÊNCIA

Os mecanismos de segurança devem ser eficientes no uso dos recursos computacionais, de forma a não afetar significativamente o desempenho do sistema ou as atividades de seus usuários.

ELO MAIS FRACO

A segurança do sistema é limitada pela segurança de seu elemento mais vulnerável, seja ele o sistema operacional, as aplicações, a conexão de rede ou o próprio usuário.



OBSERVAÇÕES IMPORTANTES

Os princípios anteriormente citados devem pautar a construção, configuração e operação de qualquer sistema computacional com requisitos de segurança. A imensa maioria dos problemas de segurança dos sistemas atuais provém da não-observação desses princípios.

AMEAÇAS

Como ameaça, pode ser considerada qualquer ação que coloque em risco as propriedades de segurança do sistema descritas na seção anterior. Alguns exemplos de ameaças às propriedades básicas de segurança seriam:

- Ameaças à confidencialidade
- Ameaças à integridade
- Ameaças à disponibilidade

AMEAÇAS À INTEGRIDADE

Um processo alterar as senhas de outros usuários, instalar programas, drivers ou módulos de núcleo maliciosos, visando obter o controle do sistema, roubar informações ou impedir o acesso de outros usuários;

AMEAÇAS À CONFIDENCIALIDADE

Um processo vasculhar as áreas de memória de outros processos, arquivos de outros usuários, tráfego de rede nas interfaces locais ou áreas do núcleo do sistema, buscando dados sensíveis como números de cartão de crédito, senhas, e-mails privados, etc.;

AMEAÇAS À DISPONIBILIDADE

Um usuário alocar para si todos os recursos do sistema, como a memória, o processador ou o espaço em disco, para impedir que outros usuários possam utilizá-lo. Obviamente, para cada ameaça.

AMEAÇAS

Obviamente, para cada ameaça possível, devem existir estruturas no sistema operacional que impeçam sua ocorrência, como controles de acesso às áreas de memória e arquivos, quotas de uso de memória e processador, verificação de autenticidade de drivers e outros softwares, etc.

As ameaças podem ou não se concretizar, dependendo da existência e da correção dos mecanismos construídos para evitá-las ou impedi-las. As ameaças podem se tornar realidade à medida em que existam vulnerabilidades que permitam sua ocorrência.

VULNERABILIDADE

Uma vulnerabilidade é um defeito ou problema presente na especificação, implementação, configuração ou operação de um software ou sistema, que possa ser explorado para violar as propriedades de segurança do mesmo.

ATAQUE

Um ataque é o ato de utilizar (ou explorar) uma vulnerabilidade para violar uma propriedade de segurança do sistema.

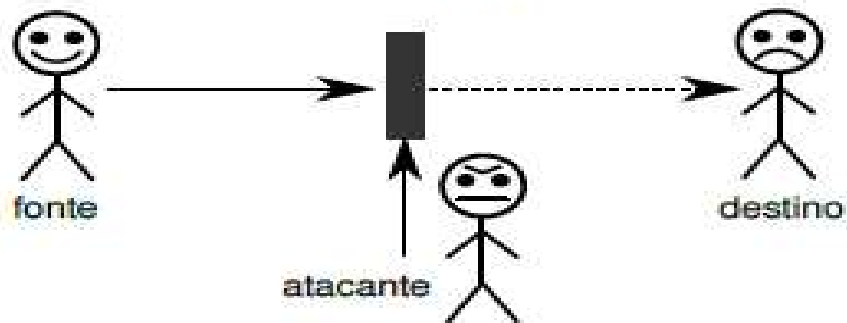


ALGUNS TIPOS DE ATAQUE

- **Interrupção** - consiste em impedir o fluxo normal das informações ou acessos; é um ataque à disponibilidade do sistema.
- **Interceptação** - consiste em obter acesso indevido a um fluxo de informações, sem necessariamente modificá-las; é um ataque à confidencialidade.
- **Modificação** - consiste em modificar de forma indevida informações ou partes do sistema, violando sua integridade.
- **Fabricação** - consiste em produzir informações falsas ou introduzir módulos ou componentes maliciosos no sistema; é um ataque à autenticidade.

ALGUNS TIPOS DE ATAQUE

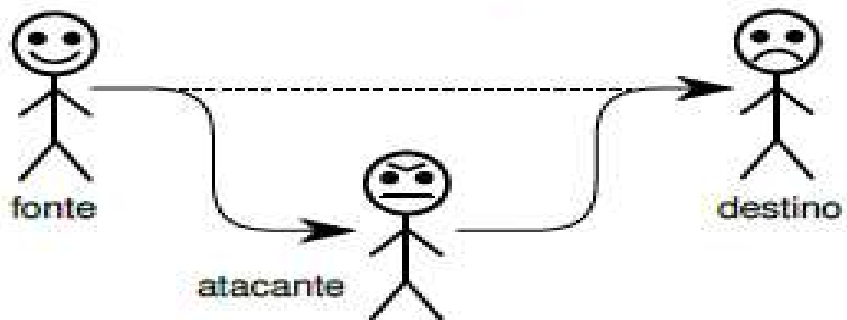
interrupção



interceptação



modificação



fabricação



ATAQUES PODEM SER

- **Passivos** - visam capturar informações confidenciais
- **Ativos** - que visam introduzir modificações no sistema para beneficiar o atacante ou impedir seu uso pelos usuários válidos
- **Locais** - quando executados por usuários válidos do sistema
- **Remotos** - quando são realizados através da rede, sem fazer uso de uma conta de usuário local. Um programa especialmente construído para explorar uma determinada vulnerabilidade de sistema e realizar um ataque é denominado exploit.

MALWARE

Denomina-se genericamente malware todo programa cuja intenção é realizar atividades ilícitas, como realizar ataques, roubar informações ou dissimular a presença de intrusos em um sistema. Existe uma grande diversidade de malwares, destinados às mais diversas finalidades [Shirey, 2000, Pfleeger and Pfleeger, 2006].

MALWARE

OBS. Existe muita confusão em relação à nomenclatura de malwares; além disso, muitos Malwares têm várias funcionalidades e se encaixam em mais de uma categoria.



MALWARE

Alguns Tipos de Malware

- Vírus
- Worm
- Trojan horse
- Exploit
- Packet snier
- Keylogger
- Rootkit
- Backdoor

MALWARE

Vírus : um vírus de computador é um trecho de código que se infiltra em programas executáveis existentes no sistema operacional, usando-os como suporte para sua execução e replicação. Quando um programa “infectado” é executado, o vírus também se executa, infectando outros executáveis e eventualmente executando outras ações danosas. Alguns tipos de vírus são programados usando macros de aplicações complexas, como editores de texto, e usam os arquivos de dados dessas aplicações como suporte. Outros tipos de vírus usam o código de inicialização dos discos e outras mídias como suporte de execução.

MALWARE

Worm - Ao contrário de um vírus, um “verme” é um programa autônomo, que se propaga sem infectar outros programas. A maioria dos vermes se propaga explorando vulnerabilidades nos serviços de rede, que os permitam invadir e instalar-se em sistemas remotos. Alguns vermes usam o sistema de e-mail como vetor de propagação, enquanto outros usam mecanismos de auto-execução de mídias removíveis (como pendrives) como mecanismo de propagação. Uma vez instalado em um sistema, o verme pode instalar spywares ou outros programas nocivos.

MALWARE

Trojan horse : O cavalo de Tróia é um programa que tem um pacote de vírus que é usado geralmente para obter informações ou executar instruções em um determinado computador.

O conceito nasceu de um simples programa que se faziam passar por esquemas de autenticação, em que o utilizador era obrigado a inserir as senhas, pensando que estas operações eram legítimas. Por exemplo, na autenticação de uma shell, poderia ser um simples programa numa conta já aberta, e o utilizador que chegasse seria forçado a introduzir a sua password. O trojan iria então guardar o password e mascarar a conta (que seria do dono do trojan) para que parecesse legítima (a conta da vítima). Entretanto, o conceito evoluiu para programas mais completos ([próximo slide](#)).

MALWARE

Trojan Horse - Os trojans atuais são disfarçados de programas legítimos, embora, diferentemente de vírus ou de worms, *não criam réplicas* de si (e esse é o motivo pelo qual o Cavalo de Tróia não é considerado um vírus). São instalados diretamente no computador. De fato, alguns trojan são programados para se auto-destruir com um comando do cliente ou depois de um determinado tempo.

Os *Trojans* atuais são divididos em duas partes:

- O servidor
- O cliente

O "servidor" se instala e se oculta no computador da vítima, normalmente dentro de algum outro arquivo. No momento que esse arquivo é executado, o computador pode ser acessado pelo cliente, que irá enviar instruções para o servidor executar certas operações no computador da vítima.

A direta tende a precisar do IP da vítima para funcionar, já a reversa tem o IP do dono do *trojan*, fazendo assim a conexão. Geralmente um trojan é instalado com o auxílio de um ataque de engenharia social, com apelos para convencer a vítima a executar o arquivo do servidor, o que muitas vezes acaba acontecendo, dada a curiosidade do internauta, como um email atraindo a pessoa a ver fotos de um artista, pedindo a instalação de um *plugin*, onde o *trojan* fica "hospedado" dentre outras.

MALWARE

Exploit - é um programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional – como o próprio sistema operativo ou serviços de interação de protocolos (**ex: servidores Web**). São geralmente elaborados por hackers como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por crackers a fim de ganhar acesso não autorizado a sistemas. Por isso muitos crackers não publicam seus exploits, conhecidos como **0days**, e o seu uso massificado deve-se aos script kiddies.

Significado de **0days** - criminosos não têm interesse em melhorar a segurança dos programas, mas apenas explorar os erros que existem. Por isso, em vez de avisar a empresa ou indivíduo responsável, eles irão tentar usar a falha para ganho próprio. Assim, a vulnerabilidade estará sendo explorada antes mesmo que uma correção esteja disponível. A falha então vira "dia zero".

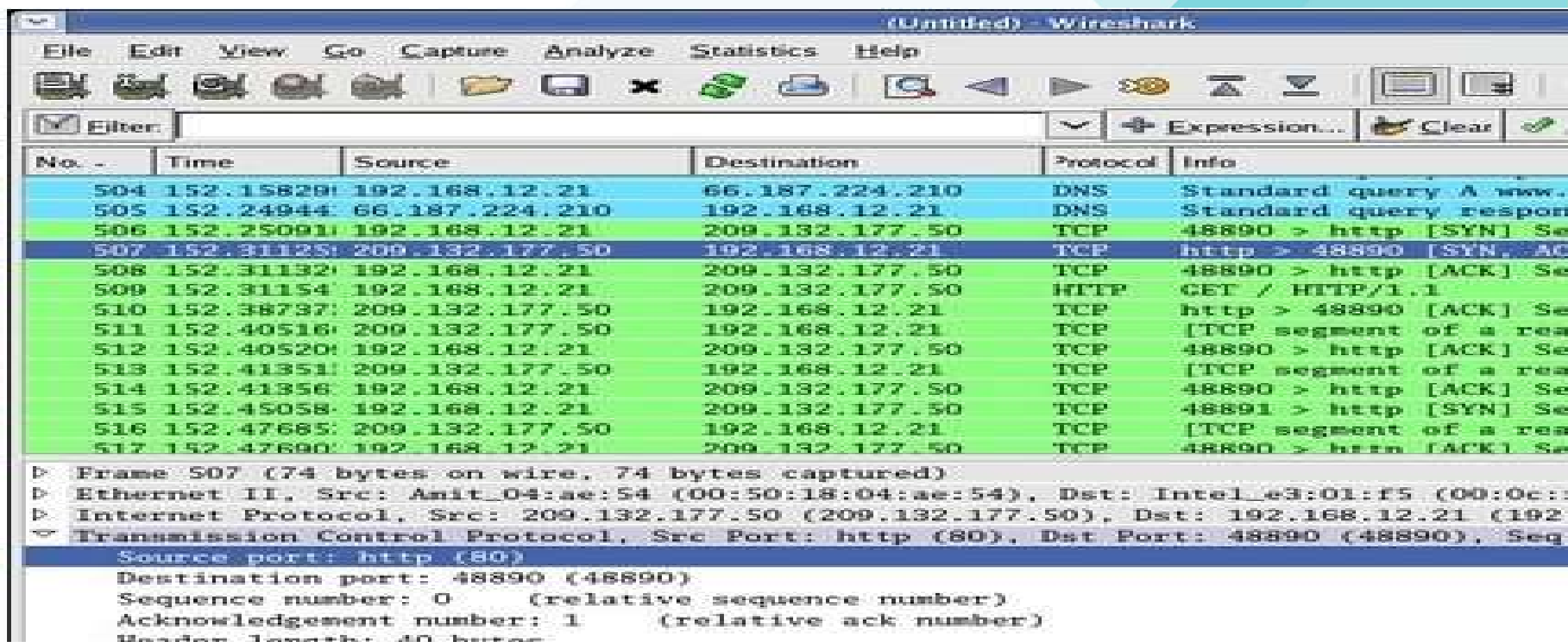
MALWARE

Packet sniffer : Esta ferramenta, constituída de um *software* ou *hardware*, é capaz de interceptar e registrar o tráfego de dados em uma rede de computadores. Conforme o fluxo de dados trafega na rede, o *sniffer* captura cada pacote e eventualmente decodifica e analisa o seu conteúdo de acordo com o protocolo definido em um RFC ou uma outra especificação.

O *sniffing* pode ser utilizado com propósitos maliciosos por invasores que tentam capturar o tráfego da rede com diversos objetivos, dentre os quais podem ser citados, obter cópias de arquivos importantes durante sua transmissão, e obter senhas que permitam estender o seu raio de penetração em um ambiente invadido ou ver as conversações em tempo real.

MALWARE

Packet sniffer - WIRESHARK



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and packet analysis. A filter bar is present with a checkmark icon and the text 'Filter:'. The main packet list table displays captured packets with columns for No., Time, Source, Destination, Protocol, and Info. Packet 507 is selected, and its details are shown in the bottom pane. The details pane shows the hierarchy: Frame 507 (74 bytes on wire, 74 bytes captured) > Ethernet II, Src: Anit_04:ae:54 (00:50:18:04:ae:54), Dst: Intel_e3:01:f5 (00:0c:29:14:01:f5) > Internet Protocol, Src: 209.132.177.50 (209.132.177.50), Dst: 192.168.12.21 (192.168.12.21) > Transmission Control Protocol, Src Port: http (80), Dst Port: 48890 (48890), Seq: 15247690. The expanded TCP section shows Source port: http (80), Destination port: 48890 (48890), Sequence number: 0 (relative sequence number), and Acknowledgement number: 1 (relative ack number).

No.	Time	Source	Destination	Protocol	Info
504	152.158290	192.168.12.21	66.187.224.210	DNS	Standard query A www
505	152.24944	66.187.224.210	192.168.12.21	DNS	Standard query response
506	152.25091	192.168.12.21	209.132.177.50	TCP	48890 > http [SYN] Seq
507	152.31125	209.132.177.50	192.168.12.21	TCP	http > 48890 [SYN, AC
508	152.31132	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq
509	152.31154	192.168.12.21	209.132.177.50	HTTP	GET / HTTP/1.1
510	152.38797	209.132.177.50	192.168.12.21	TCP	http > 48890 [ACK] Seq
511	152.40516	209.132.177.50	192.168.12.21	TCP	[TCP segment of a rea
512	152.40520	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq
513	152.41351	209.132.177.50	192.168.12.21	TCP	[TCP segment of a rea
514	152.41356	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq
515	152.45058	192.168.12.21	209.132.177.50	TCP	48891 > http [SYN] Seq
516	152.47685	209.132.177.50	192.168.12.21	TCP	[TCP segment of a rea
517	152.47690	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq

Frame 507 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Anit_04:ae:54 (00:50:18:04:ae:54), Dst: Intel_e3:01:f5 (00:0c:29:14:01:f5)
Internet Protocol, Src: 209.132.177.50 (209.132.177.50), Dst: 192.168.12.21 (192.168.12.21)
Transmission Control Protocol, Src Port: http (80), Dst Port: 48890 (48890), Seq: 15247690
Source port: http (80)
Destination port: 48890 (48890)
Sequence number: 0 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Bytes in sequence: 40 bytes

MALWARE

Packet sniffer

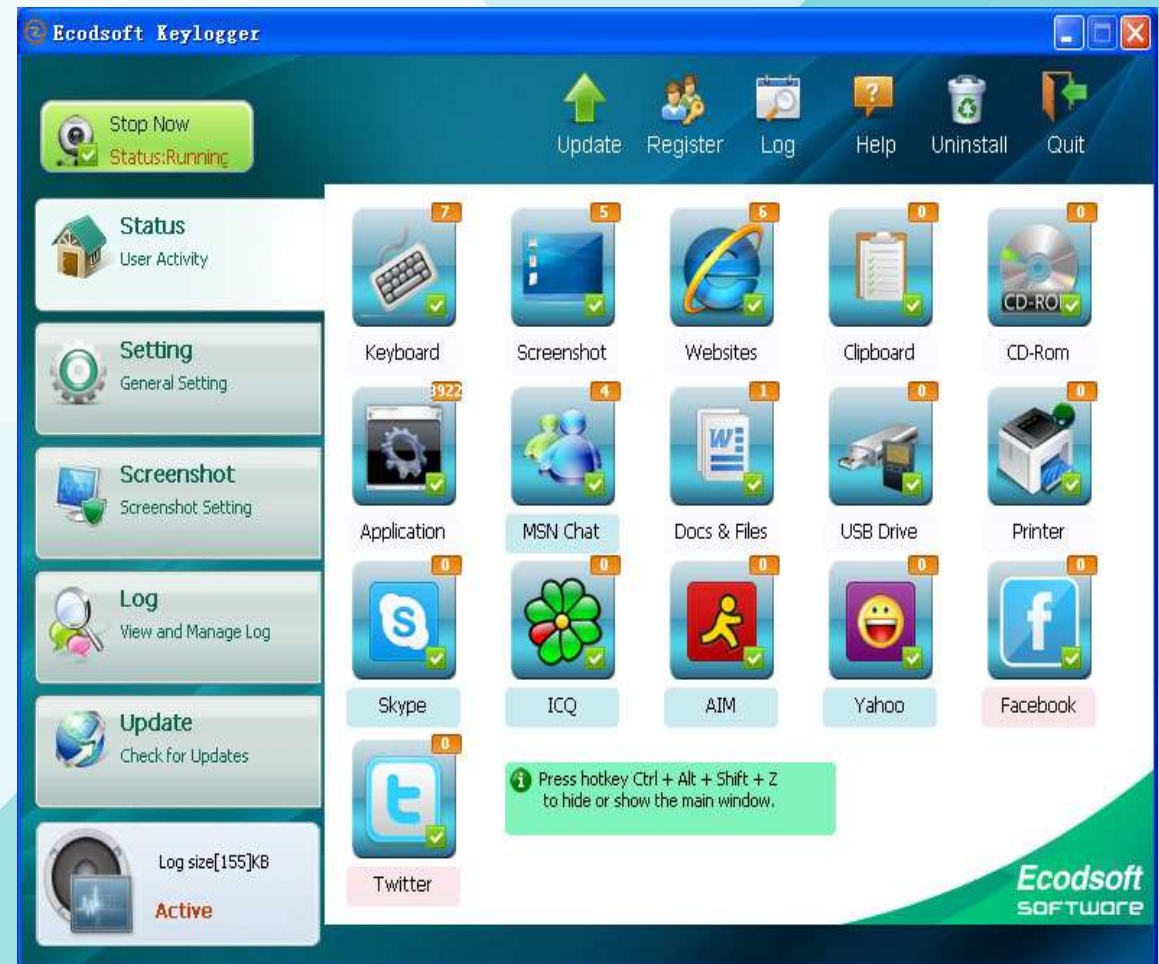
- Em redes não comutadas (ex: HUBs) os pacotes são enviados a todas as máquinas da rede, porém, as máquinas ignoram os pacotes que lhes não são destinados;
- Para que a NIC (Network Interface Card) receba todos os pacotes que chega, ela deve ser colocada num modo conhecido como “promiscuo”. Os sniffers trabalham neste modo (bem como os detectores de intrusão);
- Em redes com HUB é possível escutar todo o tráfego, em redes com SWITCHs teoricamente isto não é possível;
- Para se colocar uma NIC em modo promiscuo, os sistemas operacionais atuais exigem que se tenha permissão de administrador/root no ambiente.

MALWARE

Keylogger : software dedicado a capturar e analisar as informações digitadas pelo usuário na máquina local, sem seu conhecimento. Essas informações podem ser transferidas a um computador remoto periodicamente ou em tempo real, através da rede.

MALWARE

Keylogger



MALWARE

Rootkit : é um conjunto de programas destinado a ocultar a presença de um intruso no sistema operacional. Como princípio de funcionamento, o rootkit modifica os mecanismos do sistema operacional que mostram os processos em execução, arquivos nos discos, portas e conexões de rede, etc., para ocultar o intruso.

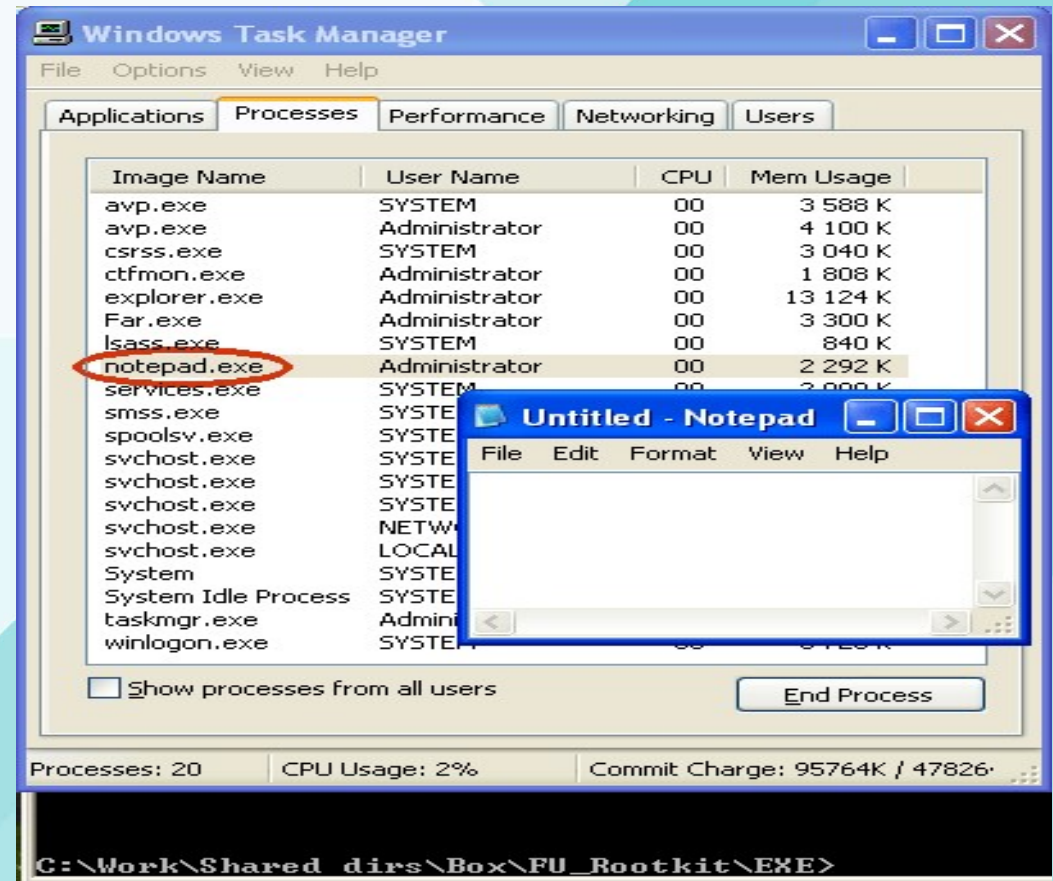
Os rootkits mais simples substituem utilitários do sistema, como ps (lista de processos), ls (arquivos), netstat (conexões de rede) e outros, por versões adulteradas que não mostrem os arquivos, processos e conexões de rede do intruso. Versões mais elaboradas de rootkits substituem bibliotecas do sistema operacional ou modificam partes do próprio núcleo, o que torna complexa sua detecção e remoção.

Malware

ROOTKIT



ssdpapi.dll WINDOWS\system32 34816
ssdpsrv.dll WINDOWS\system32 71680
ssflwbox.scr WINDOWS\system32 393216
ssmarque.scr WINDOWS\system32 20992
ssmypics.scr WINDOWS\system32 47104
ssmyst.scr WINDOWS\system32 18944
sspipes.scr WINDOWS\system32 610304
ssspl30.ocx WINDOWS\system32 177608
ssstars.scr WINDOWS\system32 14336
sstext3d.scr WINDOWS\system32 679936
Status.MPF WINDOWS\system32 63296
stclient.dll WINDOWS\system32 59392
stdole32.tlb WINDOWS\system32 7168
sti.dll WINDOWS\system32 68096
sti_ci.dll WINDOWS\system32 136704
stimon.exe WINDOWS\system32 14848
stobject.dll WINDOWS\system32 121856
storage.dll WINDOWS\system32 4208
storprop.dll WINDOWS\system32 74752
streamci.dll WINDOWS\system32 8192
strmdll.dll WINDOWS\system32 8192



Windows Task Manager

File Options View Help

Applications Processes Performance Networking Users

Image Name	User Name	CPU	Mem Usage
avp.exe	SYSTEM	00	3 588 K
avp.exe	Administrator	00	4 100 K
csrss.exe	SYSTEM	00	3 040 K
ctfmon.exe	Administrator	00	1 808 K
explorer.exe	Administrator	00	13 124 K
Far.exe	Administrator	00	3 300 K
lsass.exe	SYSTEM	00	840 K
notepad.exe	Administrator	00	2 292 K
services.exe	SYSTEM	00	2 000 K
smss.exe	SYSTEM	00	4 K
spoolsv.exe	SYSTEM	00	4 K
svchost.exe	SYSTEM	00	4 K
svchost.exe	SYSTEM	00	4 K
svchost.exe	SYSTEM	00	4 K
svchost.exe	NETW	00	4 K
svchost.exe	LOCAL	00	4 K
System	SYSTEM	00	4 K
System Idle Process	SYSTEM	00	4 K
taskmgr.exe	Admini	00	4 K
winlogon.exe	SYSTEM	00	4 K

☐ Show processes from all users

End Process

Processes: 20 CPU Usage: 2% Commit Charge: 95764K / 47826K

C:\Work\Shared dirs\Box\FU_Rootkit\EXE>

MALWARE

Backdoor : uma “porta dos fundos” é um programa que facilita a entrada posterior do atacante em um sistema já invadido. Geralmente a porta dos fundos é criada através de um processo servidor de conexões remotas (usando SSH, telnet ou um protocolo ad-hoc). Muitos backdoors são instalados a partir de trojans, vermes ou rootkits.

MALWARE

BACKDOOR



© CERT.br/NIC.br